

From: Shawn A. Geddis <geddis@apple.com>
Date: Wed, Dec 17, 2008 at 12:05
Subject: [Fed-Talk] Mac OS X 10.5.6 - Smart Card Services Update
To: Fed Talk <fed-talk@lists.apple.com>

In an effort to ensure folks understand what was included as part of the Smart Card Services Update piece of the Mac OS X 10.5.6 release, allow me to review that with you here....

Previously, we had been making available a separate universal installer (Smart Card Services Update v1.2) and all of those updates were included in the 10.5.6 update.

Smart Card Service Updates

Smart Card Services components shipped in Mac OS X 10.5.0 - 10.5.5 require specific updates to support some of the newer Smart Cards issued within the US Federal Government and improve support for a broader range of CCID compliant Smart Card Readers. Many newer cards being issued support a faster transfer protocol (T=1) and some also are hybrid cards (both CAC & PIV applets). They require a negotiation of which protocol to use (T=0 or T=1) which was not previously necessary.

PCSC

- PCSC.Framework /System/Library/Frameworks/
- pcscd /usr/sbin/

CCID Class Driver

- ifd-ccid.bundle /usr/libexec/SmartCardServices/drivers/

Smart Cards - Tokend

- CAC.tokend /System/Library/Security/tokend/
- PIV.tokend /System/Library/Security/tokend/

New CCID Class Driver

Mac OS X 10.5.6 ships with a new CCID Class Driver which supports ~90 CCID Compliant Readers. You can see all of the readers that are supported with the CCID Class Driver by looking at the collaborating Author's Open Source website at: <http://pcsclite.alioth.debian.org/ccid.html>

If you have *any* different reader than listed at the URL or supported by a pre-installed driver noted below, you would need to acquire the appropriate driver from the vendor directly.

Smart Card Reader Drivers shipped by Apple:

Directory: /usr/libexec/SmartCardServices/drivers/

Drivers: CC-PC-Card.bundle (CRYPTOCard PC-1 -- PC Card Reader)
SCR24XHndlr.bundle (SCM SCR 24X -- PC Card Reader)
ifd-ASEIIIeUSB.bundle (Athena IIIe -- USB Reader)
ifd-ccid.bundle (*NEW* CCID Class Driver -- USB Readers)
ifdok_cm4040_macos-2.0.0.bundle (OMNIKey CardMan 4040 -- PC Card Reader)

NOTE If you are using the typical SCM SCR 331(or readers based on the same mechanism), you will also need to flash that reader to be fully CCID Compliant with at least the v5.25 Firmware Update from SCM. The readers were initially issued quite a while ago and many have very old firmware which does

not conform to the CCID specification. Note that you will need access to a Windows system to flash the reader using the Utility located at the following URL:

http://www.scmmicro.com/support/pcs_downloads.php?lang=en

PKI Protected Websites

1) NMCI Users

If you are an NMCI Services user, Dennis Hayes (from EDS) continues to provide specific information to access NMCI sites. You should grab his "CAC for a Mac" document. Note though that the document

speaks of the "Smart Card Services Update v1.2" installer which is no longer needed when you have updated to Mac OS X 10.5.6.

<http://idisk.mac.com/dp.hayes-Public/>

2) DoD Smart Card Users

The Smart Card Services Update is NOT related to issues you may have had or still have in accessing some of your DoD Internet Services (Web , OWA, etc.).

Previous User Experience:

Previous to upgrading to Mac OS X 10.5.3, users were able to successfully access PKI protected Government websites using their US Federal Government Smart Cards (i.e. DoD -> CAC) without intervention, but also without knowing there were problems. In some cases, the user now needs to manually configure an association between which Certificate to use for the specific URL they are accessing.

Related Change in 10.5.3 Safari:

- Fundamental changes within Mac OS X on how Client-side Certificates are handled

Safari, Mac OS X 10.5.3: Changes in client certificate authentication
<http://support.apple.com/kb/HT1679>

User Experience:

Mac OS X 10.5.2 (and earlier) / Safari:

Safari 3 automatically sends the first available client certificate in your keychain

Mac OS X 10.5.3 (and later) / Safari:

You will be prompted to select a client certificate when server requests it.

An Identity Preference is then created for the associated URL and Cert.

Server Side Configuration Caveat:

Safari may not prompt you to select a client certificate if the server you are attempting to authenticate to is configured to *optionally* accept (rather than require) client X.509 authentication. Many of the US Federal Government web servers are configured for *optional* rather than *required*, since there is still a transition from User/Pass over to Smart Cards.

System will auto create Identity Preference *IF* Server is configured to *require* Client-side Certs

As noted in the KBase article referenced above, when accessing a website configured as *required*, Safari will prompt the user for the appropriate certificate to use for client authentication, but ONLY if it is configured as *required*.

Manually Creating Identity Preferences -- Server configured for *optional*

In this case you can force a particular client certificate to be sent by manually creating an identity preference item for the desired server authentication. Note that it is important to know the correct URL for the actual authentication process which may significantly differ from the standard login URL.

For example, if you are authentication to AKO:

The website URL is: <https://www.us.army.mil/>

The CAC Login URL is: <https://akocac.us.army.mil/>

NOTE:

It is *sometimes* best to not try and fully qualify the complete URL, but rather just include the FQDN - Fully Qualified Domain Name for the server you are authenticating to. In many cases, you should ensure you have terminated the URL with the "/" to complete the proper host specification. For example, do not just enter the above URL as <https://akocac.us.army.mil> without the trailing "/", because it will fail for you. Server Configuration changes over the last year have caused inconsistency in this behavior, so this guidance is for awareness and is not absolute in all cases.

Also, make sure that you are selecting the *proper* Certificate from the card. *Proper* means the certificate expected / required by the Server for user authentication. It may require you to check with your local Admin or help desk to determine which certificate is required for that site.

Since you are manually creating the Identity Preference, you need to ensure that you are selecting the right one. The Certificate selected is easily changed by opening up the "Identity Preference" within your default keychain using Keychain Access and selecting an alternative Certificate.

Troubleshooting:

To provide you and Apple with the ability to troubleshoot why you may still be failing to authenticate to a given server, Apple enabled a debug flag which, when enabled, will log identity preference information to the System log (/var/log/system.log).

Enable Identity Preference Debug Mode in 10.5.4 and beyond:

```
% defaults write com.apple.security LogIdentityPreferenceLookup -boolean true
```

When enabled, each identity preference lookup is written as in the following example:

Jul 1 18:12:51 /Applications/Safari.app/Contents/MacOS/Safari[386]: preferred identity: "User" found for "https://Full.Server.Name/...."

These messages might allow some to correct the host name they entered in the manually configured Identity Preference.

If you are still failing, provide these log messages along with your Reader and Card information in a bug report at:

<http://bugreport.apple.com/>

Quickest way to capture this info is to launch Terminal and execute the following command while you have your reader attached and card inserted:

```
% pcsctest
```

Select the number (typically "1") which corresponds to the reader with the card inserted,

...capture the output from this command and include in your bugreport to Apple.

Contents of the mentioned Kbase Article mentioned in this post:

- > Safari, Mac OS X 10.5.3: Changes in client certificate authentication
- > <http://support.apple.com/kb/HT1679>
- >
- >
- > Summary
- > Safari 3's handling of client certificate authentication changes in Mac OS X 10.5.3 and later.
- > This improves the security and reliability of client certificate-authenticated connections to servers.
- >
- > o Mac OS X 10.5.2 and earlier behavior: Safari 3 automatically sends the first available client certificate in your keychain to the website.
- > o Mac OS X 10.5.3 and later behavior: No client certificate is sent until you have the opportunity to select the appropriate one to use for that site. You will be prompted by Safari 3 to select a client certificate at the point where the server requests client authentication. After selecting a client certificate, the decision is remembered in your keychain as an "identity preference item", and you will not be prompted again when returning to the same site.
- >
- > Note: Safari may not prompt you to select a client certificate if a server is configured to optionally accept (rather than require) client authentication. In this case you can force a particular client certificate to be sent by creating an identity preference item for that server.
- >
- > To manually specify a client certificate be used for a particular website:
- >
- > 1. Open Keychain Access (in Applications/Utilities) and find your client certificate. Click the "My Certificates" category to easily see available client certificates.
- > 2. Control-click the certificate, then choose "New Identity Preference..." from the contextual menu.

- > 3. A sheet appears in the dialog. Type (or paste) the URL of the page that requires the certificate, exactly as it appears in Safari's location field (for example, "https://www.apache-ssl.org/cgi/cert-export").
- > 4. Note: With Mac OS X 10.5.4 or later, you may specify a partial URL to match any page on a server (for example, "https://www.apache-ssl.org/").
- > 5. Choose the certificate from the pop-up menu, then click Add to create the identity preference. (You may need to click the "All Items" category to view the newly created item.)
- >
- > To change your decision about which client certificate to use for a particular website:
- >
- > 1. Open Keychain Access (in Applications/Utilities) and find the identity preference item for the website in question. Tip: Click the "All Items" category and enter the website name in the search field in the upper right corner.
- > 2. Open the item and select a different certificate from the pop-up menu.
- > 3.
- >
- > 4. As an alternative to step 2, you can delete the identity preference item from the keychain. The next time you visit the site with Safari 3 you will be prompted to select your client certificate.

Related Messages for additional guidance

In addition to all of this, I have previously sent informative messages to the Fed-Talk list which many should find very helpful. They had the subject of:

[Discussion] 10.5.x/Smart Card/Safari Issues

[Discussion] (1) Reader and/or Card not recognized by Mac OS X 10.5*

[Discussion] (2) Card recognized, but I cannot access PKI protected Websites

[Discussion] (3) Enabling Intermediate CA Certificates - SystemCACertificates

[Discussion] (4) Support Smart Card "Types" on Mac OS X 10.5

In the near future, there will also be further good news for enhancements and access to these enhancements via an alternative location. More information will follow when appropriate.

- Shawn

Shawn Geddis 🍏 Security Consulting Engineer 🍏 Apple Enterprise